Panasonic

情シス必読！

要件整理で迷わない バックアップ製品 選定の基本

はじめに

バックアップ製品の選定は、情シスにとって避けて通れない重要課題です。しかし**「どの製品が最適か？」という問いに、万能な答えはありません**。クラウド化やSaaS利用が進む今、バックアップ対象はオンプレミスのサーバからMicrosoft 365やSalesforceなどのクラウドサービスまで広がり、さらにランサムウェア対策や運用効率といった要件も複雑化しています。
本資料では、失敗しない選定のために押さえるべき基本を体系的に整理しました。ポイントは、**セキュリティ・運用・対象の3つの観点で要件を明確化すること**です。イミュータブルやデータ隔離、多要素認証などの攻撃対策、リストア速度や感染検知機能といった運用要件、そしてクラウドやSaaS対応の可否を、チェックリスト形式でわかりやすく解説します。
「オールマイティな製品は存在しない」からこそ、自社の必須要件と任意要件を整理し、最適解を導くことが重要です。本資料が、迷わないバックアップ製品選びのご参考になれば幸いです。

この資料でわかること

1 **バックアップ製品選定に必要な要件の全体像**

2 **自社に最適な製品を見極めるためのチェックポイント**

もくじ

バックアップ製品は何を選べばいいの？

多種多様なバックアップ製品がある中、製品選定のトレンドは下記3点と言われています。ただし一概に〇×で判断できるものではなく、お客様のバックアップしたい対象やご要件によって、最適な製品が異なってきます。

製品選定の３つのトレンド

❶ 簡単・簡易

導入・運用の手間を最小限に抑え、**専門知識がなくても使いこなせる製品**が求められています

例
- ・直感的なUI/UX
- ・自動化機能
- ・簡単な初期設定

❷ 技術革新

最新技術を活用した高速化・効率化により、**ビジネスの変化に対応できる柔軟性**が重要です

例
- ・重複排除技術
- ・クラウド対応
- ・高速リストア

❸ セキュリティ

ランサムウェア対策をはじめ、バックアップデータ自体を守る機能が必須となっています

例
- ・イミュータブル
- ・多要素認証
- ・感染検知機能

バックアップの対象や自社の要件によって最適な製品が異なる

バックアップ更改の失敗事例とリスク

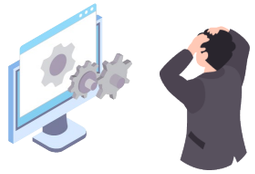
バックアップ製品の選定ミスは、データ損失や復旧遅延など、ビジネスに重大な影響を及ぼします。よくある失敗事例には下記のようなケースがあります。失敗を避けるためには、要件を具体的に定義すること・必須要件と任意要件を明確に区別し、妥協できない点を決めること・導入前にPoCを実施することなどが非常に重要になります。

よくある失敗事例

要件定義が不十分だった

「クラウド対応」という点だけで製品を選定。導入後、SaaSのバックアップに対応していないことが判明。追加で別製品を導入する必要が生じ、予算超過と運用の複雑化を招いた。

教訓 バックアップ対象を具体的に洗い出し、各対象に対応できるか詳細に確認する必要がある



セキュリティ対策が甘かった

コスト重視で製品を選定。イミュータブル機能やデータ隔離機能がない製品を導入。その結果、ランサムウェア攻撃を受け、バックアップデータも暗号化されてしまい、復旧不可能に。

教訓 セキュリティ要件は妥協せず、攻撃に対する多層防御を実現できる製品を選ぶべき

運用負荷を考慮しなかった

機能が豊富な製品を選定したが、設定が複雑で専門知識が必要であり、少人数の情シス部門では運用が困難に。バックアップの設定ミスが頻発し、いざという時にリストアできないケースが発生。

教訓 自社の運用体制（人員、スキルレベル）に合った製品を選ぶことが重要

回避するには...

- バックアップ対象、セキュリティ、運用の各要件を具体的に定義する
- 必須要件と任意要件を明確に区別し、妥協できない点を決める
- PoC（概念実証）で実際の環境での動作を確認してから導入する

バックアップの様々な要件

バックアップの主な要件は以下の通りです。バックアップ製品の種類はたくさんありますが、それぞれ特徴を持っており、お客様のご要件に合った製品を選択する必要があります。
お客様の必須要件・任意要件を明確に決めていただいた上で、〇の数が多い製品を選択すると自然と製品が絞られてきます。

❶ バックアップ対象

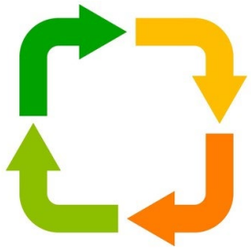
何をバックアップするのか、**対象システムやデータの種類**を明確にします

例
- オンプレミス環境
- クラウド環境
- SaaSアプリケーション
- 物理サーバ

❷ 攻撃に対する対策

バックアップデータを**どのように保護し、攻撃から守るか**を定義します

影響例
- 保管場所のセキュリティ
- イミュータブル機能
- 多要素認証
- データ隔離



❸ 運用

日常的な運用のしやすさと、**障害時**の復旧手順を考慮します

影響例
- 感染検知機能
- リストア速度
- 自動化レベル
- 監視・アラート機能

バックアップの様々な要件　-バックアップ対象-

要件の1つ目は「バックアップ対象を何にするか」です。例えばMicrosoft 365のTeamsでは、チームでの情報共有、個別チャット、会議録画などが可能ですが、バックアップ対象の要件を細かく決めておくことが大切です。取りたい内容によっては、製品が対応していない場合もあります。

バックアップ対象の例

アプリサーバ

業務アプリの設定、稼働環境、ログなど、サービス継続に必要なアプリ関連データ

DBサーバ

取引情報・顧客情報などの構造化データやメタデータ

ファイルサーバ

部門共有資料や業務文書、履歴データ、アクセス権設定などのファイル群

Microsoft 365

メール・Teamsの共有ファイル・チャット履歴・会議録画・SharePointのサイトデータ

Salesforce

商談・取引先情報、カスタムオブジェクト、メタデータ、レポート

他SaaSサービス

業務アプリごとの顧客情報、ログ、共有データなど、クラウド上で扱う各種データ一式

バックアップ対象を具体的に洗い出し、各対象に対応できるか確認しておくことが重要

バックアップの様々な要件　-攻撃に対する対策-

要件の2つ目は「攻撃に対する対策」です。具体的な要件例としてはバックアップをどのような場所に置くか、また置いた場所のセキュリティ面はどうするか、データ保全のためにどのような攻撃対策をするかがあります。稼働OSも、WindowsやLinux、独自OSなどさまざまです。

攻撃に対する対策

バックアップ保管場所

攻撃範囲に巻き込まれない保存先をどう選ぶか、物理・論理の分離度を検討

多要素認証

管理者アクションをどこまで強固に守るか、認証手段の組み合わせをどう設計するか

稼働OS

OSの攻撃耐性やメンテ性、脆弱性管理のしやすさをどう確保するか

イミュータブル

データを改ざん不能にする期間をどう設定するか、復旧要件とのバランスを確認

侵入防止機能

バックアップ環境への不正侵入をどう検知・遮断するか、必要な防御レベルを判断

データ隔離

本番とバックアップをどの程度離すか、攻撃連鎖を防ぐための分離方法を検討

セキュリティ要件は妥協せず、攻撃に対する多層防御を実現できる製品を選ぶべき

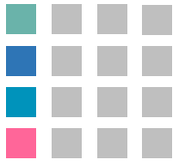
バックアップの様々な要件　-運用-

要件の3つ目は「運用」です。攻撃された場合に感染可能性をどのような仕組みで知るか、またデータの復旧の早さ等が要件として挙げられます。リストア機能は必須要件となると思いますが、スピード重視、リストア時にスキャンをする等、各社で重きを置いている要件が異なります。

運用要件の例

感染検知機能

異常な挙動をどれだけ早く正確に検知できるか、またその通知方法と精度



重複排除率

保存データをどこまで削減できるか、容量効率と処理負荷のバランス

リストア機能

どれくらいの速度と手順で復旧できるか、スキャン有無や復旧方法の柔軟性

バックアップ取得方法

フル・増分・差分をどう組み合わせるか、運用負荷や取得時間を踏まえて検討

復旧手順

障害時に迷わず復旧できるか、手順の明確さと平時の準備状況

ディスク不足時の対応

容量逼迫時にどのように動作するか、自動削除・通知・拡張の挙動はどうか

自社の運用体制（人員、スキルレベル）に合った製品を選ぶことが重要

ランサムウェア対策を重視するなら「Rubrik」

当社ではさまざまなバックアップソリューションを取り扱っていますが、「Rubrik」はランサムウェア対策を重視される企業様におすすめです。Rubrikは保存されたバックアップデータに対して一切の上書き・削除を許さない「イミュータブルファイルシステム」を採用しています。設定変更すらできない構造により、攻撃者が侵入してもバックアップを破壊できず、復旧の最後の砦として機能します。

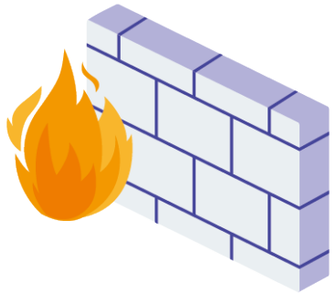
バックアップソリューション「Rubrik」の特徴

特徴 01

イミュータブル

保存されたバックアップデータに対して一切の上書き・削除を許さない「イミュータブルファイルシステム」を採用

特徴 02



論理エアギャップ

バックアップ対象と保管環境を論理的に分離する「エアギャップ構成」でバックアップ取得時以外は通信を遮断し、外部からのアクセスを防御

特徴 03

自動検知

バックアップデータ内の異常な振る舞いや暗号化の兆候を自動で検知。感染前後の状態を比較し、粒度の高い分析で「安全な復旧ポイント」を特定

特徴 04

自動バックアップ

新たに仮想マシンが追加されても、自動で保護対象に含めるため、設定漏れや運用ミスを防止

※「Rubrik」はRubrik Japan株式会社の製品です

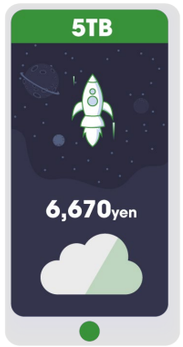
ゼロトラスト思想に基づき、バックアップの「改ざん不可」「自動復旧」「可視化」を実現

二次バックアップの保存先におすすめの「Wasabi」

二次バックアップの保存先としておすすめなのが、クラウドストレージ「Wasabi」です。Wasabiは圧倒的に低価格な点が最大の特徴であり、転送料金が無料のため予算を立てやすいというメリットもあります。ハイパフォーマンスかつ強固なセキュリティを構築しており、グローバル各社に導入されています。

クラウドストレージ「Wasabi」の特徴

特徴 01



圧倒的低価格

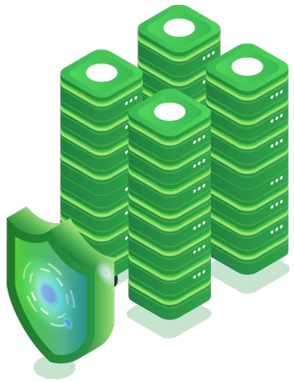
5TBで月額6,670円～。他のクラウドストレージと比較し約80%安価であり、データ転送料も無料

特徴 02

ハイパフォーマンス

Wasabi独自のテクノロジーで高速ファイルシステムを実現

特徴 03



強固なセキュリティ

AmazonS3Standardと同じ99.999999999%のオブジェクト耐久性。オブジェクトロック機能で簡単にランサムウェア対策を実現

特徴 04

AWS S3互換

Amazon S3互換APIを完全サポート。これまでS3で使用しているアプリケーションの変更が不要

※「Wasabi」はWasabi社の製品です

Wasabiは全世界80,000社に導入されているクラウドストレージ

バックアップ戦略の方向性を、ITプロが一緒に整理します

バックアップの対象や貴社のご要件によって、最適なバックアップ製品は異なります。
自社だけでは選べない！という方は、ぜひパナソニック デジタルにご相談ください。

バックアップツールや二次バックアップ先をご検討の方は、
パナソニック デジタルにお問合せください

Rubrikの詳細を見る

Wasabiの詳細を見る

バックアップ戦略の方向性について問合せする

ご連絡先

パナソニック デジタル株式会社
大阪本社 TEL：06-6906-2801 住所：〒530-0053 大阪府大阪市北区末広町2番40号
東京本社 TEL：03-5148-5634 住所：〒104-0061 東京都中央区銀座8丁目21番1号

Panasonic

